09/554518
PCT/US99/24157
WO 00/22774

SYSTEM AND METHOD OF AUTHENTICATING A KEY AND TRANSMITTING SECURE DATA

BACKGROUND OF THE INVENTION

1. Field of the invention

The present invention relates generally to computer security and more specifically to allow the authentication of a key for the transmission of secure data between computers using the key.

2. Description of the Prior Art

In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority. The private key is given only to the

requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

The private key is vital key to a user. If the private key is copied or stolen from the user, then secured data can be compromised as well as causing problems in properly authenticating the private key and the user using the private key.

Thus, it would be desirable to provide a system and method of authenticating a key so that the transmission of secure data using the key can be reliably originating from an authenticated key and/or an identifiable user.

SUMMARY OF THE INVENTION

A system and method is provided for authenticating a key of a user by decrypting an encrypted data file provided by the user with a password provided by the user into the authenticated key of the user. The encrypted data file can be stored on a RF smart card and can contain encrypted biometric data identifying the user, such as a fingerprint. An additional security measure can be used by taking a digitized biometric fingerprint scan of the user and probabilistically comparing the digitized fingerprint scan of the user with the authenticated key of the user. The user's key can then be used to securely encrypt and transmit data accordingly knowing that the key has been authenticated.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a user's key being authenticated prior to transmitting secure data over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the client computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the client computer of FIG. 2; and

FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer, according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a web server 100 and a client computer 102 connected to the Internet 110. For security purposes, the client computer 102 has a RF reader (radio frequency reader) 104 for reading a RF smart card 106 having a user's private key. The private key on the RF smart card 106 can be very long (i.e. 1000 bytes) and could include any type of biometric data, such as a digitized fingerprint of the user. The private key could be very long and any data that is encrypted using this private key would be virtually impossible to decrypt by a hacker, since this private key can be much longer than a typical private key (64 bytes) used in a

private/public key system. The client 102 also has a fingerprint scanner 108 for helping to authenticate the private key of the user. Biometric readings employed by this invention are not limited to fingerprints. Other types of biometric readings can also be used, such as the reading from the eye and analysis of the face.

FIG. 2 is a block diagram of the client computer 102 shown in FIG. 1. Computer 102 includes a CPU 202, a RAM 204, a non-volatile memory 206, an input device 208, a display 210, an Internet interface 212 for providing access to the Internet, a RF reader interface 214, and a fingerprint scanner interface 216.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the client computer 102 of FIG. 2. The non-volatile memory 206 includes an encrypt/decrypt engine 302 for encrypting and decrypting data.

The encrypt/decrypt engine 302 is programmed to encrypt and decrypt data using a password or a key. Excellent results can be obtained when using the blowfish algorithm for encryption and decryption. Other types of symmetric key encryption/decryption algorithms can also be employed within the encrypt/decrypt engine 302.

FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer in accordance with the invention. The authentication process begins at step 400. The authentication process includes three security levels, however, not every level of

security is required to authenticate the key of the user. Depending on the type of application, only one or two of the security levels may be employed.

Security level I 402 begins at step 404 where the user scans his user's RF key card 106 with the RF reader 104. Security level II 406 then begins at step 408 where the user enters his password at the client computer 102. At step 410 the data scanned from the user's RF key card is decrypted with the encrypt/decrypt engine 302 using the user's password.

At step 414, security level III 412 begins and a digitized fingerprint scan is taken from the user. At step 416 the digitized fingerprint scan is compared with the data decrypted from the RF key card. At step 418 it is determined if there is a probabilistic match between the digitized fingerprint scan and the data decrypted from the RF key card. If it is determined that there is not a match, then at step 420 the authentication of the user's key fails and is rejected. If at step 418 it is determined that there is a match, then at step 422 the user's key is authenticated. The decrypted data from the RF key card can then be used as an authenticated encryption key for sending data to a server over and unsecure network, such as the Internet.